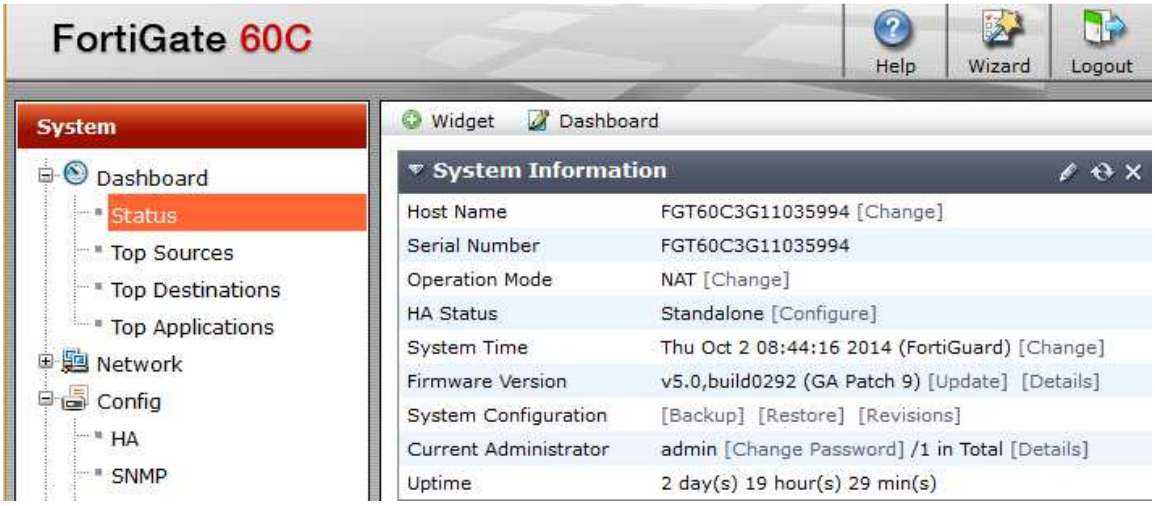
Configure a Data Link Prevention Sensor to block files by the extension.

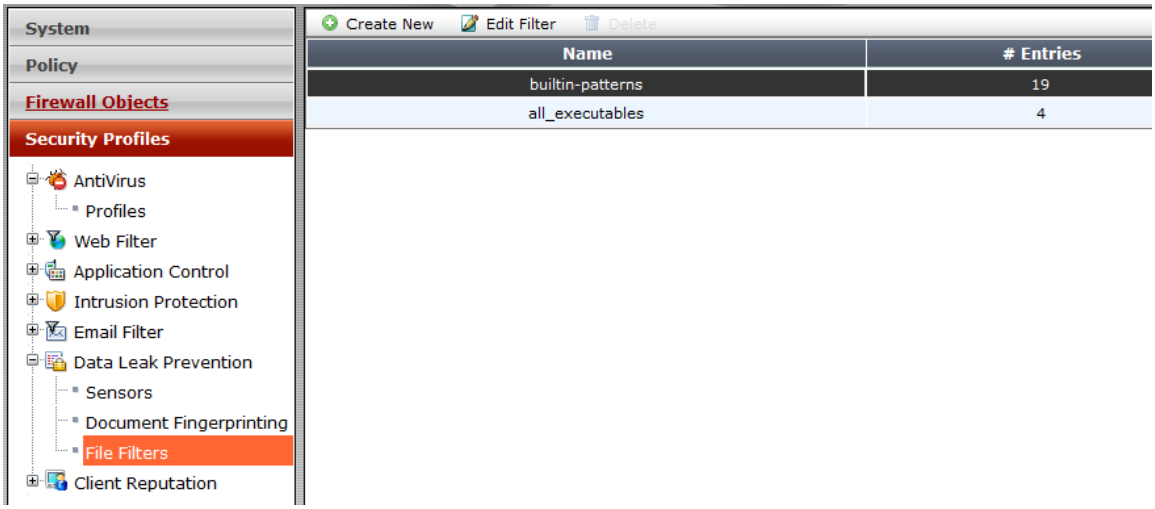
Firmware versión 5.0.9



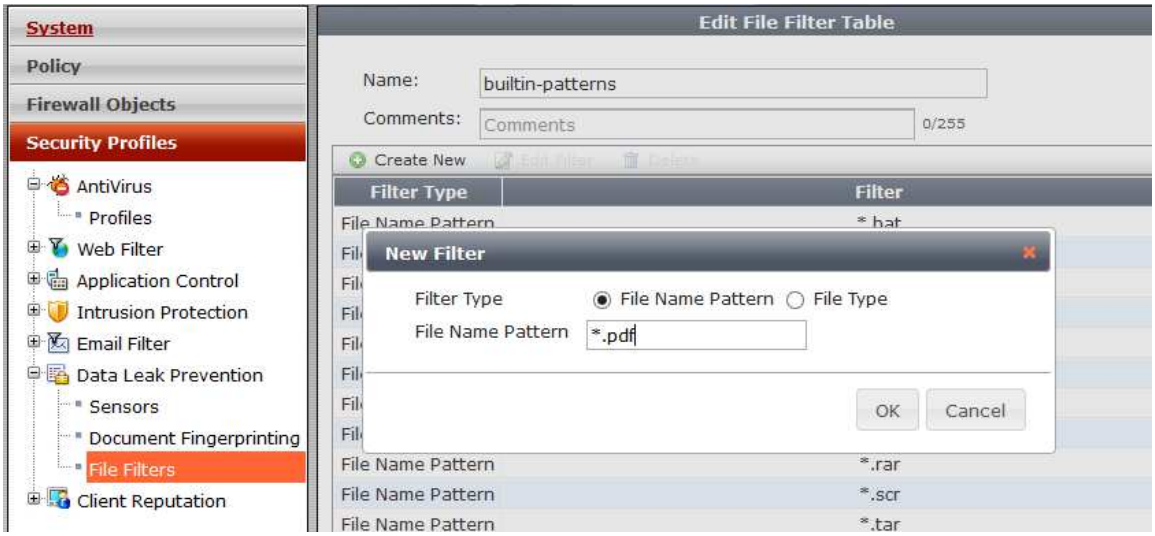
Creating a file filter, Go to:

Security Profiles> Data Leak Prevention> File Filters.

Select“ builtin-patterns” and edit.



After select; Create New and write: *.pdf



Clic Apply.

Creating a Sensor, Go to:

Security Profiles > Data Leak Prevention > Sensors.

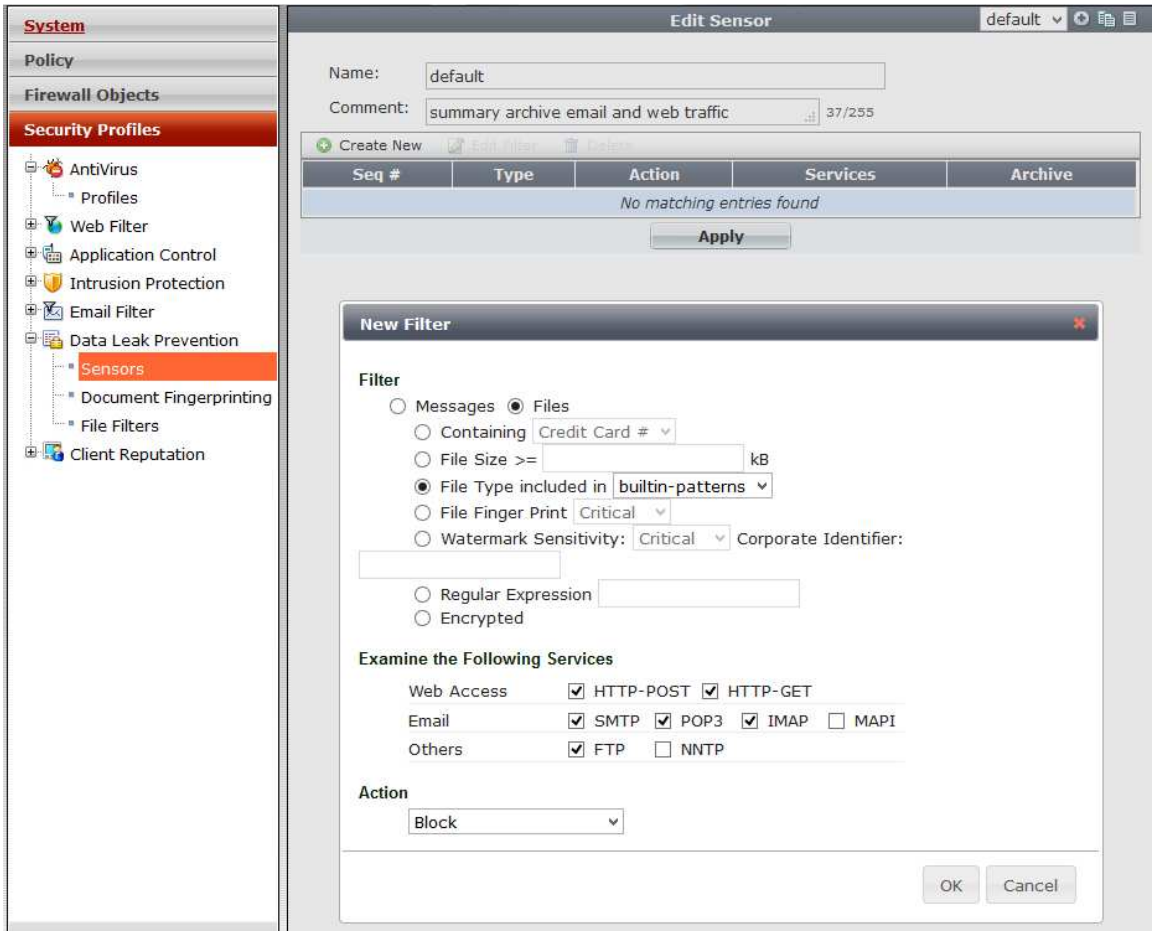
In this example we use Default Sensor.

Create New

Select Files

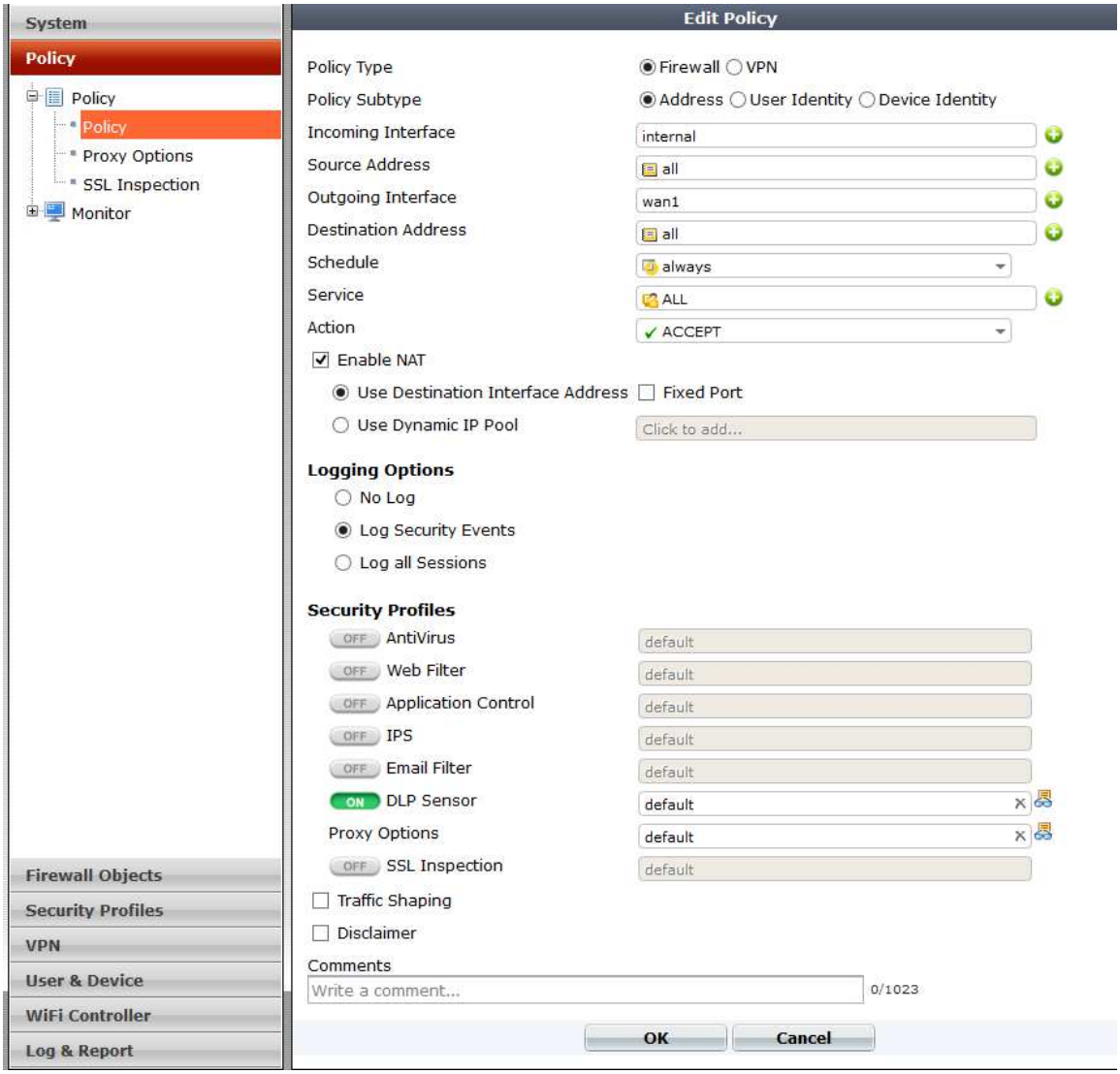
Select File Type include in: an enable builtin-patterns

In Action Select: Block


System
Policy
Firewall Objects
Security Profiles
AntiVirus
Profiles
Web Filter
Application Control
Intrusion Protection
Email Filter
Data Leak Prevention
Sensors
Document Fingerprinting
File Filters
Client Reputation
Edit Sensor
default
Name:
default
Comment:
summary archive email and web traffic
37/255
Create New
Seq #
Type
Action
Services
Archive
No matching entries found
Apply
New Filter
Filter
Messages
Files
Containing
Credit Card #
File Size >=
kB
File Type included in
builtin-patterns
File Finger Print
Critical
Watermark Sensitivity:
Critical
Corporate Identifier:
Regular Expression
Encrypted
Examine the Following Services
Web Access
HTTP-POST
HTTP-GET
Email
SMTP
POP3
IMAP
MAPI
Others
FTP
NNTP
Action
Block
OK
Cancel

OK and Apply

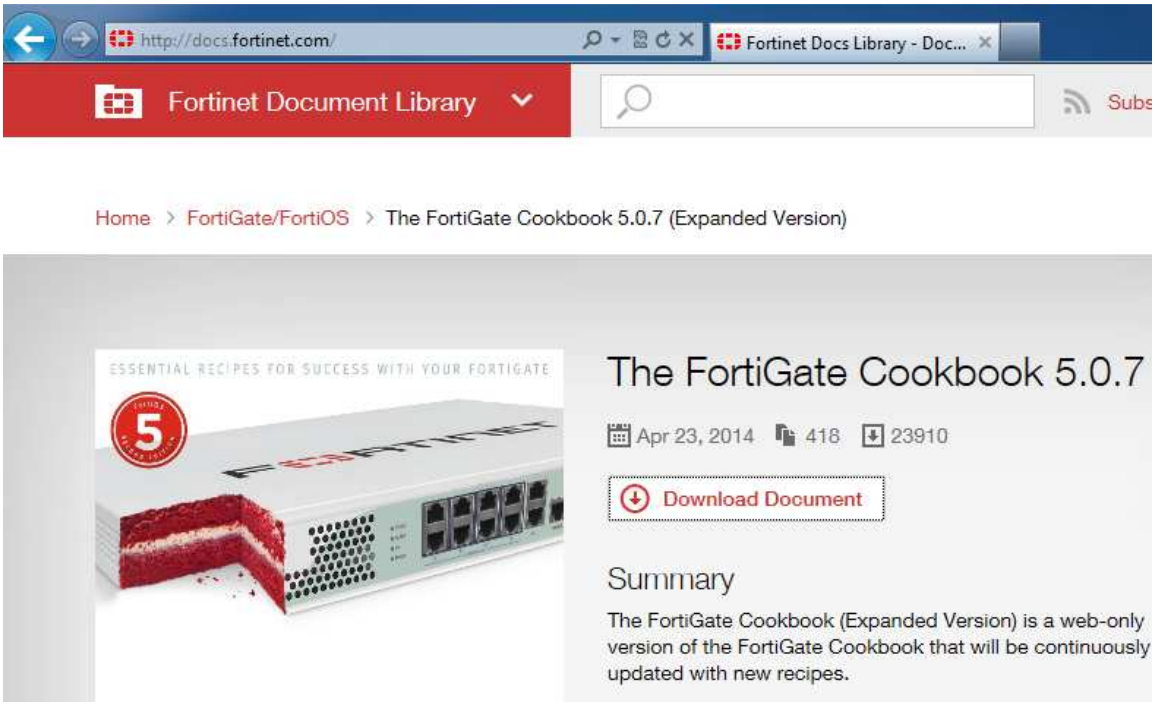
In the General Firewall Policy (you can create one for tests) enable DLP Sensor Default.

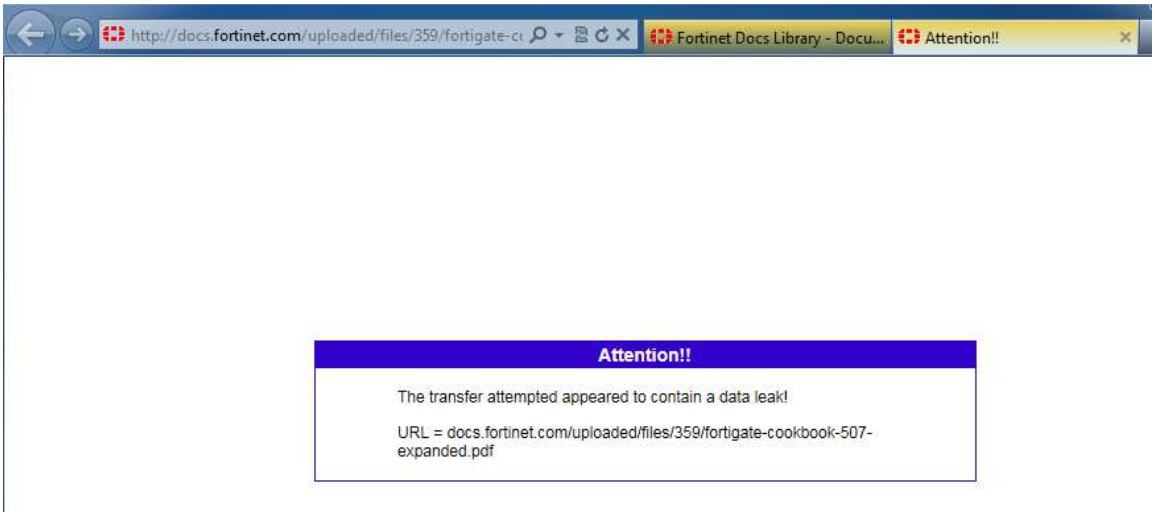


In a Laptop test open the next URL.

http://docs.fortinet.com

And try to download a PDF.





Regards.